This document is scheduled to be published in the
Federal Register on 03/23/2023 and available online at
federalregister.gov/d/2023-05925, and on **govinfo.gov**

DEPAR

Privacy Act of 1974; System of Records

AGENCY: Veterans Health Administration, Department of Veterans Affairs (VA).

ACTION: Notice of a modified system of records.

SUMMARY: Pursuant to the Privacy Act of 1974, notice is hereby given that the Department of Veterans Affairs (VA) is modifying the system of records entitled, “Income Verification Records-VA" (89VA10NB). This system is used to verify the household income of certain Veterans and, if relevant, their spouses or dependents receiving VA health care benefits. The information in this system of records is also used to validate Veterans' and their spouses' Social Security numbers; provide educational materials related to income verification; respond to Veteran and non-Veteran inquiries related to income verification; and compile management reports.

DATES: Comments on this amended system of records must be received no later than 30 days after date of publication in the *Federal Register*. If no public comment is received during the period allowed for comment or unless otherwise published in the *Federal Register* by the VA, the modified system of records will become effective a minimum of 30 days after date of publication in the *Federal Register*. If VA receives public comments, VA shall review the comments to determine whether any changes to the notice are necessary.

ADDRESSES: Comments may be submitted through www.Regulations.gov or mailed to VA Privacy Service, 810 Vermont Avenue, NW, (005R1A), Washington, DC 20420. Comments should indicate that they are submitted in response to “Income Verification Records-VA" (89VA10NB). Comments received will be available at regulations.gov for public viewing, inspection or copies.

FOR FURTHER INFORMATION CONTACT: Stephania Griffin, Veterans Health Administration (VHA) Chief Privacy Officer, Department of Veterans Affairs, 810

Vermont Avenue, NW, Washington, DC 20420; telephone (704) 245-2492 (Note: this is not a toll-free number).

SUPPLEMENTARY INFORMATION: VA is amending the system of records by revising the System Number; System Location; System Manager; Categories of Records in the System; Records Source Categories; Routine Uses of Records Maintained in the System; and Policies and Practices for Retention and Disposal of Records. VA is republishing the system notice in its entirety.

The System Number is being updated from 89VA10NB to 89VA10 to reflect the current VHA organizational routing symbol.

The System Location is being updated to remove language that shows that records are also stored at contracted locations in McLean, Virginia and Atlanta, Georgia. This section will now include language that shows that backup records are also stored at Disaster Recovery sites located in Hines, Illinois and Philadelphia, Pennsylvania.

The System Manager is being updated to remove the following language: Official responsible for policies and procedures: Chief Business Office (10NB2A), VA Central Office, 810 Vermont Avenue NW., Washington, DC 20420. Official maintaining the system: Director, Health Eligibility Center, 2957 Clairmont Road, Atlanta, Georgia 30329. Telephone number 202-461-4239. This section will now reflect the following language: VHA Member Services, Health Eligibility Center, Income Verification Division Program Office. Questions related to the Income Verification program may be referred to the Health Eligibility Center Income Verification Division by telephone at 1-800-929-8387 (this is not a toll-free number), by email at VHAHECIVDMgmt@va.gov, or postal

service at Department of Veterans Affairs, Health Eligibility Center Income Verification Division, 2957 Clairmont Road, Suite 200 Atlanta, Georgia 30329-1647.

The Categories of Records in the System is being updated to include demographics on individuals, such as name, address, date of birth and Internal Control Number (ICN).

The Records Source Categories is being updated to replace 24VA10P2 with 24VA10A7, and 147VA16 with 147VA10. Veterans and Beneficiaries Identification and Records Location Subsystem-VA" (38VA23) is being removed from this section. This section will include Internal Revenue Services (IRS) and Social Security Administration (SSA).

The language in Routine Use #7 is being updated. It previously reflected the following language: VA may disclose information in this system of records to the Department of Justice (DOJ), either on VA's initiative or in response to DOJ's request for the information, after either VA or DOJ determines that such information is relevant to DOJ's representation of the United States or any of its components in legal proceedings before a court or adjudicative body, provided that, in each case, the agency also determines prior to disclosure that disclosure of the records to DOJ is a use of the information contained in the records that is compatible with the purpose for which VA collected the records. VA, on its own initiative, may disclose records in this system of records in legal proceedings before a court or administrative body after determining that the disclosure of the records to the court or administrative body is a use of the information contained in the records that is compatible with the purpose for which VA collected the records.

Routine Use #7 will now read as follows: DOJ, Litigation, Administrative Proceeding: To the Department of Justice (DoJ), or in a proceeding before a court,

adjudicative body, or other administrative body before which VA is authorized to appear, when:

(a) VA or any component thereof;

(b) Any VA employee in his or her official capacity;

(c) Any VA employee in his or her official capacity where DoJ has agreed to represent the employee; or

(d) The United States, where VA determines that litigation is likely to affect the agency or any of its components,

is a party to such proceedings or has an interest in such proceedings, and VA determines that use of such records is relevant and necessary to the proceedings.

Routine use #20 is being added to state, “To another Federal agency or Federal entity, when VA determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.”

Policies and Practices for Retention and Disposal of Records is being updated to remove the previous language in that section and replace it with: Records in this system are retained and disposed of in accordance with the scheduled approved by the Archivist Records Control Schedule (RCS) 10-1, Item Numbers 1250.1, 1250.2, 1250.3. (DAA-0015-2018-0001, items 0001-0003)

The Report of Intent to Amend a System of Records Notice and an advance copy of the system notice have been sent to the appropriate Congressional committees and to the Director of the Office of Management and Budget (OMB) as required by 5 U.S.C.

552a(r) (Privacy Act) and guidelines issued by OMB (65 FR 77677), December 12, 2000.

Signing Authority

The Senior Agency Official for Privacy, or designee, approved this document and authorized the undersigned to sign and submit the document to the Office of the Federal Register for publication electronically as an official document of the Department of Veterans Affairs. Kurt D. DelBene, Assistant Secretary for Information and Technology and Chief Information Officer, approved this document on February 10, 2023 for publication.

Dated: March 17, 2023.

Amy L. Rose,

Program Analyst,

VA Privacy Service,

Office of Information Security,

Office of Information and Technology,

Department of Veterans Affairs.

SYSTEM NAME AND NUMBER: “Income Verification Records-VA" (89VA10)

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: Records are located at VA's Health Eligibility Center (HEC) in Atlanta, Georgia and the Austin Information Technology Center (AITC) in Austin, Texas. Back up records are also stored at Disaster Recovery sites located in Hines, Illinois and Philadelphia, Pennsylvania.

SYSTEM MANAGER(S): Official responsible for policies and procedures: VHA Member Services, Health Eligibility Center, Income Verification Division Program Office. Questions related to the Income Verification program may be referred to the Health Eligibility Center Income Verification Division by telephone at 1-800-929-8387 (this is not a toll-free number), by email at VHAHECIVDMgmt@va.gov, or postal service at Department of Veterans Affairs, Health Eligibility Center Income Verification Division, 2957 Clairmont Road, Suite 200 Atlanta, Georgia 30329-1647.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 38 U.S.C. Sections 501(a), 1705, 1710, 1722, and 5317.

PURPOSE(S) OF THE SYSTEM: The purpose of these records is to verify the household income of certain Veterans and, if relevant, their spouses or dependents receiving VA health care benefits. The information in this system of records is also used to validate Veterans' and their spouses' Social Security numbers; provide educational materials related to income verification; respond to Veteran and non-Veteran inquiries related to income verification; and compile management reports.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: These records include information on Veterans who have applied for or have received VA health care benefits under 38 U.S.C 17; Veterans' spouses and other dependents as provided for in other provisions of 38 U.S.C.

CATEGORIES OF RECORDS IN THE SYSTEM: The category of records in the system includes:

Federal Tax Information (FTI) and Social Security information generated as a result of computer matching activity with records from the Internal Revenue Services (IRS) and Social Security Administration (SSA). The records may also include, but are not limited to, demographics on individuals, such as name, address, date of birth and Internal Control Number (ICN); correspondence between HEC, Veterans, their family members, and Veterans' representatives such as Veterans Service Officers (VSO); copies of death certificates; Notice of Separation; disability award letters; IRS documents (e.g., Form 1040s, Form 1099s, W-2s); workers compensation forms; and various annual earnings statements, as well as pay stubs and miscellaneous receipts.

Note: VA may not disclose to any person in any manner any document that contains FTI received from IRS or SSA in accordance with the Internal Revenue Code (IRC) 26 U.S.C. 6103(l)(7). In addition, VA may not allow access to FTI by any contractor or subcontractor.

RECORD SOURCE CATEGORIES: Information in this system of records may be provided by the applicant, applicant's spouse or other family members; accredited representatives or friends; employers and other payers of earned income; financial institutions and other payers of unearned income; health insurance carriers; other Federal agencies, such as IRS and SSA; "Patient Medical Records-VA" (24VA10A7); "Enrollment and Eligibility Records-VA" (147VA10); and "VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA"(58VA21/22/28)).

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES: To the extent that records contained in the system include information protected by 45 CFR parts 160 and 164, *i.e.*, individually identifiable health information of VHA or any of its business associates, and 38 U.S.C. 7332; *i.e.*, medical treatment information related to drug abuse, alcoholism or alcohol abuse, sickle cell anemia, or infection with the human immunodeficiency virus, that information cannot be disclosed under a routine use unless there is also specific statutory authority in both 38 U.S.C. 7332 and 45 CFR parts 160, 161, and 164.

1. Congress: To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.
2. Claims Representatives: To accredited service organizations, VA-approved claim agents, and attorneys acting under a declaration of representation, except FTI, so that these individuals can aid claimants in the preparation, presentation, and prosecution of claims under the laws administered by VA upon the request of the claimant and provided that the disclosure is limited to information relevant to a claim, such as the name, address, the basis and nature of a claim, amount of benefit payment information, medical information, and military service and active duty separation information.
3. Law Enforcement: To a Federal, state, local, territorial, tribal, or foreign law enforcement authority or other appropriate entity charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing such law, except FTI, provided that the disclosure, is limited to information that, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature. The disclosure of the names and

addresses of Veterans and their dependents from VA records under this routine use must also comply with the provisions of 38 U.S.C. 5701.

4. Guardians, Courts, for Incompetent Veterans: To a court, magistrate, or administrative tribunal, except FTI, in matters of guardianship, inquests, and commitments; to private attorneys representing Veterans rated incompetent in conjunction with issuance of Certificates of Incompetency; or to probation and parole officers in connection with court-required duties.

5. Guardians Ad Litem, for Representation: To a fiduciary or guardian ad litem in relation to his or her representation of a claimant in any legal proceeding as relevant and necessary, except FTI, to fulfill the duties of the fiduciary or guardian ad litem.

6. Attorneys, Insurers, Employers: To attorneys, insurance companies, employers, third parties liable or potentially liable under health plan contracts, and courts, boards, or commissions as relevant and necessary, except FTI, to aid VA in the preparation, presentation, and prosecution of claims authorized by law.

7. DOJ, Litigation, Administrative Proceeding: To the Department of Justice (DoJ), or in a proceeding before a court, adjudicative body, or other administrative body before which VA is authorized to appear, when:

(a) VA or any component thereof;

(b) Any VA employee in his or her official capacity;

(c) Any VA employee in his or her individual capacity where DoJ has agreed to represent the employee; or

(d) The United States, where VA determines that litigation is likely to affect the agency or any of its components,

is a party to such proceedings or has an interest in such proceedings, and VA determines that use of such records is relevant and necessary to the proceedings.

8. NARA: To the National Archives and Records Administration (NARA), except FTI, in records management inspections conducted under 44 U.S.C. 2904 and 2906, or other functions authorized by laws and policies governing NARA operations and VA records management responsibilities.

9. Consumer Reporting Agencies: To a consumer reporting agency, except FTI, for the purpose of locating the individual, obtaining a consumer report to determine the ability of the individual to repay an indebtedness to the United States, or assisting in the collection of such indebtedness, provided that the provisions of 38 U.S.C. 5701(g)(2) and (4) have been met, provided that the disclosure is limited to information that is reasonably necessary to identify such individual or concerning that individual's indebtedness to the United States by virtue of the person's participation in a benefits program administered by the Department.

10. Treasury, to Report Waived Debt as Income: To the Department of the Treasury as a report of income under 26 U.S.C. 61(a)(12), provided that the disclosure is limited to information concerning an individual's indebtedness that is waived under 38 U.S.C. 3102, compromised under 4 CFR part 103, otherwise forgiven, or for which the applicable statute of limitations for enforcing collection has expired.

11. Federal Agencies, Security Review Purposes: To other source Federal agencies, except FTI, for information security review purposes who are parties to computer matching agreements involving the information maintained in this system, but only to the extent that the information is necessary and relevant to the review.

12. Reported Payers of Earned, Unearned Income: To reported payers of earned or unearned income in order to verify the identifier address, income paid, period of employment, and health insurance information provided on the means test, and to

confirm income and demographic data provided by other Federal agencies during income verification computer matching.

13. Federal Agencies, for Computer Matches: To other Federal agencies, except FTI, for the purpose of conducting computer matches to obtain information, to determine or verify eligibility of Veterans receiving VA benefits or medical care under title 38, U.S.C.

14. SSA, HHS, for SSN Validation: To the Social Security Administration and the Department of Health and Human Services for the purpose of conducting computer matches to obtain information to validate the Social Security numbers maintained in VA records.

15. Contractors: To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for VA, when reasonably necessary to accomplish an agency function related to the records. Note: This routine use does not authorize disclosure of FTI received from the IRS or the SSA to contractors or subcontractors.

16. Data Breach Response and Remediation, for VA: To appropriate agencies, entities, and persons when (1) VA suspects or has confirmed that there has been a breach of the system of records; (2) VA has determined that as a result of the suspected or confirmed breach there is a risk to individuals, VA (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, or persons is reasonably necessary to assist in connection with VA efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

17. MSPB: To the Merit Systems Protection Board (MSPB), except FTI, in connection with appeals, special studies of the civil service and other merit systems, review of rules and regulations, investigation of alleged or possible prohibited personnel practices, and

such other functions promulgated in 5 U.S.C. 1205 and 1206, or as otherwise authorized by law.

18. FLRA: To the Federal Labor Relations Authority (FLRA), except FTI, in connection with the investigation and resolution of allegations of unfair labor practices, the resolution of exceptions to arbitration awards when a question of material fact is raised; matters before the Federal Service Impasses Panel; and the investigation of representation petitions and the conduct or supervision of representation elections.

19. Federal Agencies, Fraud and Abuse: To other Federal agencies to assist such agencies in preventing and detecting possible fraud or abuse by individuals in their operations and programs.

20. Data Breach Response and Remediation, for Another Federal Agency: To another Federal agency or Federal entity, when VA determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Records are currently maintained on magnetic tape, magnetic disk, optical disk, and paper at secure off-site facilities in Atlanta, Georgia and Austin, Texas. In January 2013, VA implemented a new electronic data transmission process called Direct Connect, which is a secure VPN tunnel to transmit and receive Veterans' household income from IRS. It only affects the means in which the data is transmitted; it does not affect the storage of the data.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records (or information contained in records) maintained on paper documents are indexed and are retrieved by the applicant's name, Social Security number or case number and filed in case order number. Automated records are indexed and retrieved by the Veteran's name, Social Security number, Internal Control Number, or case number. The spouse's name or Social Security number may be retrieved from the automated income verification record.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Records in this system are retained and disposed of in accordance with the schedule approved by the Archivist, VA Records Control Schedule (RCS) 10-1, Item Numbers 1250.1, 1250.2, 1250.3. (DAA-0015-2018-0001, items 0001-0003).

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

1. Electronic data transmissions between VA health care facilities, HEC, and AITC are safeguarded by using VA's secure wide area network. The transmission of electronic data between SSA and AITC is safeguarded through the use of a secured, encrypted connection. Back-up of magnetic media containing FTI is transported between AITC and the off-site location in a locked storage container by an off-site vendor. Vendor personnel do not have key access to the locked container. The locked storage container is stored in a safe in a secured room at the off-site storage location. Access to the secured room and the safe is limited to authorized VA Information Technology staff only.

2. The software programs at HEC, AITC, and VA health care facilities automatically flag records or events for transmission via electronic messages based upon functionality requirements. The recipients of the messages are controlled and/or assigned to the mail

group based on their role or position. Server jobs at each facility run continuously to check for incoming and outgoing data to be transmitted which needs to be parsed to files on the receiving end. All messages containing data transmissions include header information that is used for validation purposes. Consistency checks in the software are used to validate the transmission, and electronic acknowledgment messages are returned to the sending application. The VA Office of Cyber Security has oversight responsibility for planning and implementing computer security.

3. Working spaces and record storage areas at the HEC are secured during all business hours, as well as during non-business hours. All entrance doors require an electronic pass card, issued by the HEC Personal Card Issuer, for entry when unlocked, and entry doors are locked outside normal business hours. The card has restricted access capability, which allows restriction of unauthorized personnel to secured areas. Visitors are required to present identification and sign-in at a specified location. Visitors are issued a pass card which allows access to non-sensitive areas and are escorted by staff through restricted areas. At the end of the visit, visitors are required to turn in their card. The building is equipped with an intrusion alarm system which is activated during non-business hours. This alarm system is monitored by a private security service vendor. The HEC office space occupied by employees with access to Veteran records is secured with an electronic locking system, which requires a card for entry and exit of that office space. Access to the AITC is generally restricted to AITC staff, VA Headquarters employees, custodial personnel, Federal Protective Service, and authorized operational personnel through electronic locking devices. All other persons gaining access to the computer rooms are escorted.

4. A number of other security measures are implemented to enhance security and safeguard of electronic records such as automatic timeout after a short period of

inactivity and device locking after a pre-set number of invalid logon attempts, for example.

5. Electronic data, except FTI, is transmitted from HEC and AITC to VA health care facilities over VA secure wide area network.

6. Employees at the health care facility level do not have access to FTI, nor do they have the ability to edit or view income tests received from HEC as a result of the income match with IRS.

7. Only specific key staff and the ISO are authorized access to the computer room. Programmer access to AITC and HEC databases, which contain FTI, is restricted only to staff whose official duties require that level of access. Contractor staff are not authorized access to the production database.

8. On-line data, including FTI, reside on magnetic media in AITC computer room which are highly secured. Backup media are stored in a combination lock safe in a secured room within the same building and access to the safe is restricted to the IT staff. Backup media are stored by an off-site media storage vendor who picks up the media on a weekly basis from HEC and AITC and returns the media to the off-site storage via a locked storage container. Vendor personnel do not have key access to the locked container.

9. Any sensitive information that may be downloaded to a personal computer or printed to hard copy format is provided the same level of security as the electronic records. All paper documents and informal notations containing sensitive data are shredded prior to disposal. All magnetic media (primary computer system) and personal computer disks are degaussed prior to disposal or released off site for repair.

10. HEC and AITC fully comply with the Tax Information Security Guidelines for Federal, State and Local Agencies (Department of Treasury IRS Publication 1075) as it relates to access and protection of such data. These guidelines define the management of magnetic media, paper and electronic records, and physical and electronic security of the data.

11. All new HEC employees receive initial information security and privacy training and refresher training are provided to all employees on an annual basis. HEC's ISO performs an Annual Information Security (AIS) audit. This annual audit includes the primary computer information system, the telecommunication system, and local area networks. Additionally, the IRS performs periodic on-site inspections to ensure the appropriate level of security is maintained for FTI. HEC and AITC's ISO and AIS administrator additionally perform periodic reviews to ensure security of the system and databases.

12. Identification codes and codes used to access HEC automated communications systems and records systems, as well as security profiles and possible security violations, are maintained on magnetic media in a secure environment by the HEC ISO. For contingency purposes, database back-ups on removable magnetic media are stored off-site by a licensed and bonded media storage vendor.

13. VA field facilities do not receive FTI from AITC or HEC.

14. Contractors and subcontractors are required to adhere to HEC's safeguard and security requirements.

Access:

1. In accordance with national and locally established data security procedures, access to the HEC Legacy system and the Enrollment Database is controlled by unique entry codes (access and verification codes). The user's verification code is set to be changed automatically every 90 days. User access to data is controlled by role-based access as determined necessary by supervisory and information security staff as well as by management of option menus available to the employee. Determination of such access is based upon the role or position of the employee and functionality necessary to perform the employee's assigned duties.

2. On an annual basis, employees are required to sign a computer access agreement acknowledging their understanding of confidentiality requirements. In addition, all employees receive annual privacy awareness and information security training. Access to electronic records is deactivated when no longer required for official duties. Recurring monitors are in place to ensure compliance with nationally and locally established security measures.

3. Access to the AITC is generally restricted to AITC staff, VA Headquarters employees, custodial personnel, Federal Protective Service, and authorized operational personnel through electronic locking devices.

4. Specific key staffs are authorized access to HEC computer room and all other persons gaining access to the computer rooms are escorted. Programmer access to the information systems is restricted only to staff whose official duties require that level of access.

RECORD ACCESS PROCEDURES: Individuals seeking information on the existence and content of records in this system pertaining to them should contact the system manager in writing as indicated above. A request for access to records must contain the

requester's full name, address, telephone number, be signed by the requester, and describe the records sought in sufficient detail to enable VA personnel to locate them with a reasonable amount of effort.

CONTESTING RECORD PROCEDURES: Individuals seeking to contest or amend records in this system pertaining to them should contact the system manager in writing as indicated above. A request to contest or amend records must state clearly and concisely what record is being contested, the reasons for contesting it, and the proposed amendment to the record.

NOTIFICATION PROCEDURES: Generalized notice is provided by the publication of this notice. For specific notice, see Record Access Procedure, above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

HISTORY: 59 FR 8677 (February 23, 1994), 66 FR 27752 (May 18, 2001), 73 FR 26192 (May 8, 2008), 78 FR 76897 (December 19, 2013).

[FR Doc. 2023-05925 Filed: 3/22/2023 8:45 am; Publication Date: 3/23/2023]